UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF TEXAS

CORPUS CHRISTI DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER: (1) AUTHORIZING THE INSTALLATION AND USE OF A PEN REGISTER AND TRAP AND TRACE DEVICE; (2) AUTHORIZING RELEASE OF SUBSCRIBER AND OTHER INFORMATION; AND, (3) AUTHORIZING THE DISCLOSURE OF LOCATION-BASED SERVICES	§	Case No. 2:07mc127 (UNDER SEAL)

APPLICATION

The United States of America, by and through the undersigned Assistant United States Attorney, applies for a multi-part order authorizing (i) the installation and use of a pen register and trap and trace device; (ii) the disclosure of stored wire and electronic transactional records; and, (iii) the disclosure of location-based electronic communications data. In support of this application, Applicant states the following:

1. AUTHORITY TO SEEK ORDER. Applicant is an "attorney for the Government" as defined by Fed. R. Crim. P. 1(b)(1)(B) and, therefore, may apply for an order authorizing the installation and use of a pen register and trap and trace device and the disclosure of stored wire and electronic transactional records. 18 U.S.C. § 3122(a)(1), 3127(5) and 2703(c)(1)(B) and (d).

2. CERTIFICATION OF MATERIALITY AND FACTUAL BACKGROUND. Applicant certifies that the Drug Enforcement Administration (hereinafter, the "**Investigative Agency**") is conducting an ongoing criminal investigation regarding violations of 21 U.S.C. §841 and 846 by Monica **SANCHEZ** (hereinafter, "**Subject**") and others. Furthermore, the Applicant believes that **Subject** uses the electronic communications device bearing mobile telephone number **956-534-3886** with International Mobile Subscriber Identifier (IMSI) number **310260452037028** (hereinafter, the "**Target Device**"), which receives communications service through T-Mobile (hereinafter, "**Provider**") and is subscribed to Janet A. LUNA at McAllen, Texas. The Applicant also believes that the information likely to be obtained from the pen register and trap & trace device is relevant to the aforementioned investigation and will ultimately assist with identifying the role of the **Subject** within the drug trafficking organization. 18 U.S.C. § 3122(b)(1) & (2). By way of specific and articulable facts necessary to substantiate a request for stored wire and electronic transactional records under 18 U.S.C. § 2703(d), and a statement of probable cause necessary to substantiate a request for the authorization and use of an electronic tracking device under Fed. R. Crim. P. 41(d)(1), Applicant offers the Affidavit of DEA Special Agent Patrick Hartig (hereafter, "**Affiant**"), which is attached hereto and incorporated by reference into this Application.

3. PEN/TRAP REQUEST. Pursuant to 18 U.S.C. § 3123(a)(1), Applicant requests the Court issue an order authorizing the installation and use of a pen register[1] (including "post-cut-through dialed digits")[2] and trap and trace[3] device. In accordance with 18 U.S.C. § 3121(c) and express Department of Justice Policy, Applicant has informed the **Investigative Agency** and its agents conducting this investigation that they shall use technology reasonably available to restrict the recording or decoding of electronic or other impulses to the dialing, routing, addressing and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communication; and that no affirmative use of any such information may be made.

---

[1] A "pen register" is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication ..." 18 U.S.C. § 3127(3). This includes dialing, routing, addressing, or signaling information transmitted over the communication service provider's network by a two-way radio feature (including, but not limited to, Nextel's "Direct Connect/Direct Dispatch," Verizon Wireless' "Push to Talk," Sprint's "ReadyLink," or any other comparable service, irrespective of trade-name). *In re CALEA Second Report & Order*, FCC Docket No. 97-213 (Aug. 31, 1999) at ¶ 21. Information transmitted by the two-way radio feature will not disclose content of the call.

[2] "Post-cut-through dialed digits," also called "dialed digit extraction features," are any digits dialed from the Target Device after the initial call setup is completed and are necessary to identify, *inter alia*, the true destination of a call made with a calling card. Pursuant to the limitations of 18 U.S.C. § 3121(c) and to the extent any additional digits constitute content, the United States shall not attempt to decode such information for any affirmative investigative purpose.

[3] A "trap and trace device" is "a device or process that captures the incoming electronic or other impulses which identify the originating number" or other identifiers "reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information not include the contents of any communication." 18 U.S.C. § 3127(4). As with a pen register, this includes information captured for any two-way radio feature.

4. TRANSACTIONAL AND STORED RECORDS REQUEST. Pursuant to 18 U.S.C.§2703(c) and 2703(d) and 47 U.S.C.§1002, Applicant requests the Court issue an order directing **Provider** to disclose or provide the following, upon oral or written demand of the **Investigative Agency**:

a. Subscriber records and other information for the **Target Device** and for all published, non-published, or unlisted dialing, routing, addressing, or signaling information identified pursuant to the proposed order, being limited to:

(1) name and address;
(2) local and long distance telephone connection records, or records of session times and durations;
(3) length of service (including start date) and types of service utilized;
(4) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address and any other telephone, instrument or subscriber number or identity associated with the same master account;
(5) date of birth;
(6) social security number;
(7) driver's license (state and number);
(8) contact names and numbers, and
(9) employment information;

b. Any and all changes (including additions, deletions, and transfers) in service regarding the **Target Device**, including changed telephone numbers (MDN or MIN/MSID), network addresses (IMSI, IP and UFMI), equipment changes (e.g. ESN, IMEI and SIM)[4] and subscriber information changes (published, non-published, listed, or unlisted);

[4] MDN is the Mobile Directory Number, or the number by which a subscriber and those calling a subscriber know a telephone number. MIN is Mobile Identification Number, also known as a Mobile Subscriber

c. For the **Target Device**, records or other information pertaining to its subscriber or customer, including historical call detail records[5] and historical cell-site information[6] (including any two-way radio feature mode) and the means and source of payment for service.

d. For the **Target Device**, and pursuant also to 18 U.S.C§3123(a)(1) and 3127(3), records or other information pertaining to subscriber(s) or customer(s), including prospective cell-site information, provided to the **Investigative Agency** on a

---

Identity (MSID), or the 10-digit routing number through which telecommunications providers route calls. It is frequently the same as the MDN. Its use was brought about by the local number portability laws that allow customers to take their phone numbers to another provider. Thus, a MIN will always be a 10-digit phone number that was originally licensed to a telecommunications provider (or one of it's acquisitions) and will never be the same as the MDN *if* the subscriber "ported" or carried their number away from its original licensee. IMSI is the International Mobile Subscriber Identity, or a 16-digit number that identifies subscribers on a GSM (e.g. Cingular & T-Mobile) or iDEN (Nextel) network by Mobile Country Code, Mobile Network Code and a nine-digit subscriber identifier. IP is the Internet Protocol address and is used in routing communications through internet-based telecommunications systems. UFMI is Universal Member Fleet Identifier and is the address used to route "direct-connect" type connections. ESN is Electronic Serial Number, and is the identifier assigned to CDMA (e.g. Verizon Wireless, Sprint PCS) handsets and older protocols (TDMA and analog). IMEI is International Mobile Equipment Identity and is the GSM equivalent of an ESN. SIM is the Subscriber Identity Module, which is the chip used in GSM and iDEN handsets that contains the IMSI, IP and UFMI addresses and other user-data, and is readily transferable between handsets without the provider's agreement or knowledge.

[5] "Call detail records" are similar to toll records (i.e. historical telephone records of telephone activity, usually listing outgoing calls and date, time, and duration of each call), which are made and retained in the ordinary course of business. "Call detail records" is the term used when referring to toll records of mobile telephones (vice "hard-line," or landline, telephones) that also include local calls and may also include a record of incoming calls. Additionally information may include the cell-site, and sometime sector, used by the mobile telephone at the beginning and/or end of a call.

[6] A cell-site is located in a geographic area within which wireless service is supported through radio signaling to and from antenna tower(s) operated by a service provider. Cell-sites are located throughout the United States. Mobile telephones that are powered on or off or change switching offices will register or deregister their availability with a cellular network. The registration process is the technical means by which the network identifies the subscriber, validates the account and determines where to route subsequent call traffic. This exchange occurs in the ordinary course of business on a dedicated "control channel" that is clearly separate from that used for call content (i.e. audio, text messages, pictures), which occurs on a separate dedicated "voice channel." As used herein, "cell-site information" refers categorically to data associated with registration of the Target-Device with the tower location through which the mobile telephone connects to a provider's physical communications network. Cell-site information is typically captured at both beginning and end of a call (but not in-between) and at power-up or power-down.

continuous basis contemporaneous with call origination and call termination. Specific disclosure of cell-site information will assist law enforcement in identifying the approximate physical location of the **Target Device** but will not disclose content of the calls. As used by law enforcement, cell-site data is the means by which law enforcement determines, based on records maintained, captured and recorded by the telecommunications providers in the ordinary course of business, the first or last physical location through which a call or connection enters or leaves a telecommunications provider's infrastructure and is routed through the Public Switched Telephone Network (PSTN). Thus, this information is akin to determining the physical location where a landline telecommunications provider's copper wires terminate (also known as an "appearance point") in providing wired phone service to a specific subscriber.

5. REQUEST FOR DISCLOSURE OF LOCATION-BASED DATA. Pursuant to 18 U.S.C§ 2703(c)(1)(B) and (d) and 3123(a)(1) and 3127(3) and consistent with the probable-cause evidentiary standard articulated by Fed. R. Crim. P. 41 and set forth in the attached Affidavit, Applicant requests the Court issue an Order authorizing the **Investigative Agency** to require the **Provider** to disclose location-based data that will assist law enforcement in determining the location of the **Target Device** (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the

location of the third-party Provider's infrastructure).[7] This request for location-based data includes the request for an order directing Provider to employ and to disclose the

[7] The government does not concede that probable cause is legally required in order to receive cell site data contemporaneous with pen/trap data. Succinctly, the government asserts that cell-site information at the beginning and end of a call constitutes "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" under the clear definition of a pen register. 18 U.S.C. § 3127(3). Such information *would indisputably be* available under a standalone pen register order—but for the requirement of CALEA § 103(a)(2)(B), codified at 47 U.S.C. § 1002(a)(2)(B)("with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices...such call-identifying information shall not include any information that may disclose the physical location of the subscriber[.]). Thus, CALEA imposes an unspecified—and, deductively, higher—evidentiary burden when the government seeks to obtain "real time" information that "disclose[s] the physical location of the subscriber." (emphasis added).

That the disclosure of a cell site number and that cell-site's physical tower location constitutes disclosure of a subscriber's "physical location" is doubtful. Rather, cell-site data discloses only the physical location of a fixed antenna tower that belongs not to the *subscriber*, but to a third party telecommunications provider. And to allay any concern about the "private" nature of that tower's location...cell site towers are always visually observable from the "public highway." Clearly, disclosure of a subscriber's physical location must be something much more precise...and unique to *that* subscriber. *See, e.g. In re Application of the United States*, 2006 U.S. Dist. LEXIS 6976 (S.D. W. Va. Feb. 17, 2006) ("user" of phone who is not the "subscriber" enjoys no protection under the CALEA limitation on location information and government may, thus, obtain real-time cell sites with a pen register, alone).

Nonetheless, conservatively assuming that receipt of "real-time" cell-site data might disclose a subscriber's "physical location" in broad and vague fashion, the government believes this higher evidentiary burden is met by offering "specific and articulable facts showing that there are reasonable grounds to believe that the...records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d)(this has come to be known as the "hybrid theory" and is supported by the contemporaneous passage of the PATRIOT ACT's modification of the definition of a pen register to include "routing, addressing or signaling."); *accord, In re Application of the United States*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); *In the Matter of the Application of the United States*, 2006 U.S. Dist. LEXIS 3392, No. 06-5021M-01, 2006 WL 244270 (W.D. La. Jan. 26, 2006); *In re Application for an* Order, No. S-06-SW-0041 (E.D. Cal Mar. 15, 2006)(unreported). Importantly, the silent majority of magistrate and district courts that routinely grant pen/trap/cell orders under the combined authority of Pen/Trap and SCA continue to do so without resort to publishing decisions affirming their current practice...permitting this minority view to appear more pervasive than it is.

For those courts that reject the government's evidentiary threshold analysis or that find cell-site disclosure to constitute disclosure of a subscriber's physical location in some manner contrary to a constitutionally protected privacy interest or Congressional authorization, prospective and contemporaneous cell-site data is alternatively sought based on probable cause. *See In re Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *In re United States for an Order Authorizing the Use of a Pen Register*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134 (D.D.C. 2006); *In the Matter of the Application of the United States*, 2006 U.S. Dist. LEXIS 6737, No. 06 MISC.004, 2006 WL 243017 (E.D. Wis. Jan. 17, 2006); *In the Matter of the Application of the United States*, 2006 U.S. Dist. LEXIS 7653, No. 06-MJ-506, 2006 WL 354289 (W.D.N.Y. Feb. 15, 2006); *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register*, 402 F. Supp. 2d 597 (D. Md. 2005)(position clarified in 2006 U.S. Dist. LEXIS 7345 (D. Md. Feb. 27, 2006)).

results (through any means reasonably available) of any and all available location-based services, including but not limited to real time cell-site data and those "Enhanced-911" services developed by the **Provider** in order to comply with the provisions of 47 C.F.R.§20.18.[8] The requested order should contain a provision, identical to that found at 18 U.S.C.§2703(e) and 3124(d), that no suit shall lie against Provider for complying with the Court's order and should be valid for a period of sixty (60) days, consistent with the duration authorized by the pen register.

6. PROVIDER ASSISTANCE & COMPENSATION. Applicant requests further that **Provider** and all other providers of wire or electronic communication service, landlord, custodian, or other person furnish the Investigating Agency unobtrusively and with a minimum of interference to services all information, facilities, and technical assistance necessary to accomplish the installation of the pen register and trap and trace device; and that such providers be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance. 18 U.S.C.§3124(a), (b) and (c).

---

[8] Deductively, the Federal Communications Commission (FCC) does not consider cell-site data sufficient to identify a subscriber's "physical location" for public safety purposes...which explains why the FCC has required cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls. By the end of 2005, carriers using handset-based location technology will be required to locate cell phones within 50 meters for 67% of calls, and 150 meters for 95% of calls. Highlighting the difference between E-911 data, which locates the subscriber's device, and cell site data, which identifies the provider's infrastructure access point, there is no provision in the pen-trap statutes or CALEA to deliver E-911 information to law enforcement on a contemporaneous or recurring basis. In sharp contrast to the cell-site data created by a subscriber who knowingly [and, following *Smith v. Maryland*, 442 U.S. 735 (1979), who *voluntarily* creates *non-private*] records each and every time he chooses to use his phone, the deployment and use of "E-911" tools in situations where the handset user does not actually dial "911" might implicate the highest of electronic surveillance evidentiary standards—probable cause.

7. DELIVERY OF RECORDS. Applicant further requests that, upon request of the Investigative Agency, all records and information required to be provided pursuant to the proposed order be provided in a commercially reasonable electronic format specified by the Investigative Agency; and that those records be delivered forthwith via electronic mail (unless delivery under the current CALEA delivery protocol is possible and requested) to the email address specified by the agent serving the proposed order. 47 U.S.C.§1002(a).

8. CONTINUATION OF SERVICES. Applicant further requests, because it is necessary to advance the purposes of this investigation, that the proposed order direct **Provider** not to terminate or restrict service to the **Target Device**; provided that, upon notice to the **Investigative Agency** that service would otherwise be terminated for non-payment pursuant to routine billing practices, the **Investigative Agency** timely agrees in writing to assume financial responsibility for all services provided to the **Target Device** after termination would otherwise have been effectuated and continuing to the earlier of the **Investigative Agency's** written notice to terminate service or to the expiration of the proposed order (and any extensions thereof). Such request includes the authority for the **Investigative Agency** to reactivate service that has already been restricted or terminated.

9. APPLICABILITY AND DURATION OF REQUESTED ORDER. Applicant finally requests that the proposed order, upon service, shall apply to any person or

entity providing wire or electronic communication service in the United States whose assistance may facilitate its execution (including any internet service provider or other electronic communications provider providing voice-over IP telephony [VoIP]);[9] and that whenever served on any person or entity not specifically named therein, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served. 18 U.S.C. 3123(a)(1). Applicant requests that, pursuant to 18 U.S.C.§3123(b)(1)(C), the proposed order apply not only on the **Target Device**, but also on any changed telephone number(s) (MDN or MIN/MSID) or network addresses (IMSI, IP and UFMI) subsequently assigned to the same equipment (ESN, IMEI and SIM); and to any changed equipment subsequently assigned to the same telephone numbers(s) or network addresses; including any subsequent changes, irrespective of whether any changes occur consecutively or simultaneously, within the period authorized by the order. Applicant requests, further, that the proposed order be effective in all respects for the sixty (60) days following its execution and, with respect to stored and transactional records, effective also for the sixty (60) days preceding[10] its execution. 18 U.S.C.§3123(c) and 2703(d).

---

[9] VoIP is essentially a type of hardware and software that allows people to use the internet as a transmission medium for telephone calls. In general, this means sending voice information in the form of digital packets of information rather than sending it through the traditional public switch telephone network.

[10] Communications common carriers are required to maintain for 18 months the name address, number calling, number called, date, time and duration of all billed calls. 47 CFR § 42.6.

10. NONDISCLOSURE & SEALING. Pursuant to 18 U.S.C. §2705(b), 3123(d), and 3103a(b), Applicant further requests that the proposed order direct the **Provider**, and all other telecommunications providers, persons or entities providing service to the **Target Device** who are obligated by the proposed order to provide assistance to the **Investigative Agency**, not to disclose in any manner, directly or indirectly, by any action or inaction, to the subscriber(s) for the **Target Device**, the occupant of said premises, the subscriber of the incoming calls to or outgoing calls from the **Target Device**, or to any other person, the existence of the proposed order, in full or redacted form, the existence of the pen register or trap and trace device or the existence of this investigation, unless otherwise ordered by this Court; and that the identity of the **Subject** may be redacted from any copy of the proposed order to be served on any service provider or other person; and further that this application any order entered in connection therewith be SEALED for a period extending at least to the date of **Subject's** arrest or dismissal of the underlying arrest warrant, whichever comes first. Specifically, disclosure of the requested order and investigation would likely result in continued flight from prosecution, a modification of the **Subject's** activities or the activities of those, with whom **Subject** communicates and associates, or the destruction or tampering of evidence; and would otherwise seriously jeopardize the investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on October, ~~XX~~ 23 2007, at Corpus Christi, Texas.

Patti Booth
Assistant United States Attorney
800 N. Shoreline Blvd., Suite 500
Corpus Christi, Texas 78401
Tel: (361) 888-3111
Fax: (361) 888-3200